

Decode-and-Forward Relay Beamforming with Secret and Non-Secret Messages

Sanjay Vishwakarma and A. Chockalingam

Email: sanjay@ece.iisc.ernet.in, achockal@ece.iisc.ernet.in

Department of ECE, Indian Institute of Science, Bangalore 560012

Abstract—In this paper, we study beamforming in decode-and-forward (DF) relaying using multiple relays, where the source node sends a secret message as well as a non-secret message to the destination node in the presence of multiple non-colluding eavesdroppers. The non-secret message is transmitted at a fixed rate R_0 and requires no protection from the eavesdroppers, whereas the secret message needs to be protected from the eavesdroppers. The source and relays operate under a total power constraint. We find the optimum source powers and weights of the relays for both secret and non-secret messages which maximize the worst case secrecy rate for the secret message as well as meet the information rate constraint R_0 for the non-secret message. We solve this problem for the cases when (i) perfect channel state information (CSI) of all links is known, and (ii) only the statistical CSI of the eavesdroppers links and perfect CSI of other links are known.

keywords: Cooperative relaying, physical layer security, secret and non-secret messages, secrecy rate, multiple eavesdroppers.

I. INTRODUCTION

The foundation for secure communication using physical layer techniques was laid by Wyner in his work in [1], where the idea of secrecy rate and secrecy capacity for the wire-tap channel was introduced. The work was later extended to the broadcast channel and the Gaussian channel in [2] and [3], respectively. The broadcast nature of wireless transmissions makes them vulnerable to eavesdropping. Several works on secure wireless communication using single and multiple antennas have been reported in the literature, e.g., [4]–[7]. Cooperative relays which act as distributed antennas can be used to improve the secrecy rate performance. Secrecy rates under cooperative relaying have been studied, e.g., [11]–[15].

In [2], simultaneous transmission of a private message to receiver 1 at rate R_1 and a common message to both the receivers at rate R_0 for two discrete memoryless channels with common input was considered. Recently, the work in [2] has been extended to MIMO broadcast channel with confidential and common messages in [8]–[10]. Motivated by the above works, in this paper, we consider communication of secret and non-secret messages between a source-destination pair, aided by multiple decode-and-forward (DF) relays, in the presence of multiple non-colluding eavesdroppers. Both the secret and non-secret messages are intended for the destination. While the secret message needs to be protected from the eavesdroppers, the non-secret message need not be. The non-secret message is sent at a fixed rate R_0 . There is a total power constraint on the source and relays powers. In this setting, our aim is to find

the optimum source powers and relay weights (beamforming vectors) for the secret and non-secret messages. The objective is to maximize the worst case secrecy rate for the secret message and to meet the information rate constraint R_0 for the non-secret message. We solve this problem for two cases of channel state information (CSI) assumption. In the first case, perfect CSI of all links is assumed. In the second case, only the statistical CSI of the eavesdroppers links and perfect CSI of other links are assumed to be known.

Notations: $\mathbf{A} \in \mathbb{C}^{N_1 \times N_2}$ implies that \mathbf{A} is a complex matrix of dimension $N_1 \times N_2$. $\mathbf{A} \succeq \mathbf{0}$ denotes that \mathbf{A} is a positive semidefinite matrix. Transpose and complex conjugate transpose operations are denoted by $[\cdot]^T$ and $[\cdot]^*$, respectively. $\|\cdot\|$ denotes 2-norm operation. $\mathbb{E}[\cdot]$ denotes the expectation operator.

II. SYSTEM MODEL

Consider a DF cooperative relaying scheme which consists of a source node S , N relay nodes $\{R_1, R_2, \dots, R_N\}$, an intended destination node D , and J non-colluding eavesdropper nodes $\{E_1, E_2, \dots, E_J\}$. The system model is shown in Fig. 1. In addition to the links from relays to destination node and relays to eavesdropper nodes, we assume direct links from source to destination node and source to eavesdropper nodes. The complex fading channel gains between the source to relays are denoted by $\gamma = [\gamma_1, \gamma_2, \dots, \gamma_N] \in \mathbb{C}^{1 \times N}$. Likewise, the channel gains between the relays to destination and the relays to j th eavesdropper are denoted by $\alpha = [\alpha_1, \alpha_2, \dots, \alpha_N] \in \mathbb{C}^{1 \times N}$ and $\beta_j = [\beta_{1j}, \beta_{2j}, \dots, \beta_{Nj}] \in \mathbb{C}^{1 \times N}$, respectively, where $j = 1, 2, \dots, J$. The channel gains on the direct links from the source to destination and the source to j th eavesdropper are denoted by α_0 and β_{0j} , respectively.

Let P_T denote the total transmit power budget in the system (i.e., source power plus relays power). The communication between source S and destination D happens in two hops. Each hop is divided into n channel uses. In the first hop of transmission, the source S transmits two independent messages W_0 and W_1 which are equiprobable over $\{1, 2, \dots, 2^{2nR_0}\}$ and $\{1, 2, \dots, 2^{2nR_s}\}$, respectively. W_0 is the non-secret message to be conveyed to the destination at a fixed information rate R_0 which need not be protected from E_j s. W_1 is the secret message which has to be conveyed to the destination at some rate R_s with perfect secrecy [7], i.e., W_1 needs to be protected from all E_j s. For each W_0 drawn equiprobably from the set $\{1, 2, \dots, 2^{2nR_0}\}$, the source S maps W_0 to

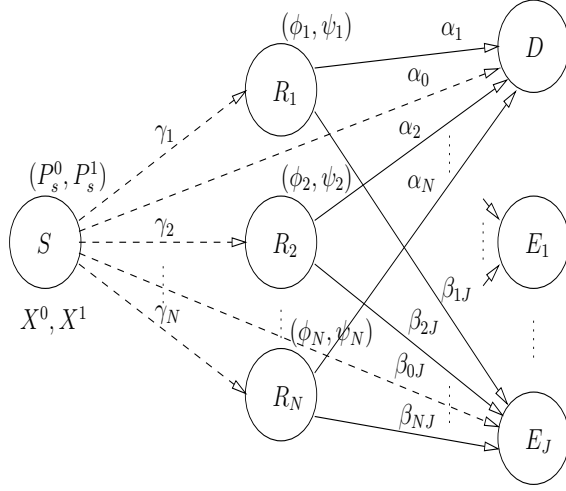


Fig. 1. DF relay beamforming with secret and non-secret messages.

an iid ($\sim \mathcal{CN}(0,1)$) codeword $X_1^0, X_2^0, \dots, X_n^0$ of length n . Similarly, for each W_1 drawn equiprobably from the set $\{1, 2, \dots, 2^{2nR_s}\}$, the source S , using a stochastic encoder, maps W_1 to an iid ($\sim \mathcal{CN}(0,1)$) codeword $X_1^1, X_2^1, \dots, X_n^1$ of length n . Let P_s^0 and P_s^1 denote the source transmit powers corresponding to the codewords $X_1^0, X_2^0, \dots, X_n^0$ and $X_1^1, X_2^1, \dots, X_n^1$, respectively. In the k th ($1 \leq k \leq n$) channel use, the source transmits the sum of the weighted symbols, i.e., $\sqrt{P_s^0}X_k^0 + \sqrt{P_s^1}X_k^1$. In the following, we will use X^0 and X^1 to denote the symbols in the codewords $X_1^0, X_2^0, \dots, X_n^0$ and $X_1^1, X_2^1, \dots, X_n^1$, respectively.

In the second hop of transmission, relays retransmit the decoded symbols X^0 and X^1 to the destination D . Let $\phi = [\phi_1, \phi_2, \dots, \phi_N]^T \in \mathbb{C}^{N \times 1}$ and $\psi = [\psi_1, \psi_2, \dots, \psi_N]^T \in \mathbb{C}^{N \times 1}$ denote the complex weights applied by the relays corresponding to the transmit symbols X^0 and X^1 , respectively. The i th ($1 \leq i \leq N$) relay transmits the sum of the weighted symbols which is $\phi_i X^0 + \psi_i X^1$.

Let y_{R_i} , y_{D_1} , and $y_{E_{1j}}$ denote the received signals at the i th relay, destination D , and j th eavesdropper E_j , respectively, in the first hop of transmission. In the second hop of transmission, the received signals at the destination and j th eavesdropper are denoted by y_{D_2} and $y_{E_{2j}}$, respectively. We then have

$$y_{R_i} = \sqrt{P_s^0}\gamma_i X^0 + \sqrt{P_s^1}\gamma_i X^1 + \eta_{R_i}, \quad \forall i = 1, 2, \dots, N, \quad (1)$$

$$y_{D_1} = \sqrt{P_s^0}\alpha_0 X^0 + \sqrt{P_s^1}\alpha_0 X^1 + \eta_{D_1}, \quad (2)$$

$$y_{E_{1j}} = \sqrt{P_s^0}\beta_{0j} X^0 + \sqrt{P_s^1}\beta_{0j} X^1 + \eta_{E_{1j}}, \quad \forall j = 1, 2, \dots, J, \quad (3)$$

$$y_{D_2} = \alpha\phi X^0 + \alpha\psi X^1 + \eta_{D_2}, \quad (4)$$

$$y_{E_{2j}} = \beta_j\phi X^0 + \beta_j\psi X^1 + \eta_{E_{2j}}, \quad \forall j = 1, 2, \dots, J. \quad (5)$$

The noise components, η 's, are assumed to be iid $\mathcal{CN}(0, N_0)$.

III. BEAMFORMING WITH SECRET AND NON-SECRET MESSAGES - KNOWN CSI ON ALL LINKS

In this section, we assume perfect knowledge of the CSI on all links. This assumption can be valid in scenarios where the eavesdroppers are also legitimate users in the network. Since the symbol X^0 is transmitted at information rate R_0 irrespective of X^1 , treating X^1 as noise, relays will be able to decode X^0 if $\forall i = 1, 2, \dots, N$,

$$\frac{1}{2}I(X^0; y_{R_i}) = \frac{1}{2}\log_2 \left(1 + \frac{P_s^0 |\gamma_i|^2}{N_0 + P_s^1 |\gamma_i|^2} \right) \geq R_0, \quad (6)$$

where (6) is derived using (1) and the factor $1/2$ appears because of the two hops. Similarly, using (2) and (4), the destination D will be able to decode X^0 if

$$\frac{1}{2}I(X^0; y_{D_1}, y_{D_2}) = \frac{1}{2}\log_2 \left(1 + \frac{P_s^0 |\alpha_0|^2}{N_0 + P_s^1 |\alpha_0|^2} + \frac{\phi^* \alpha^* \alpha \phi}{N_0 + \psi^* \alpha^* \alpha \psi} \right) \geq R_0. \quad (7)$$

Using (1) and with the knowledge of the symbol X^0 , the information rate for X^1 at the i th relay is

$$\frac{1}{2}I(X^1; y_{R_i}|X^0) = \frac{1}{2}\log_2 \left(1 + \frac{P_s^1 |\gamma_i|^2}{N_0} \right). \quad (8)$$

Similarly, using (2) and (4), the information rate for X^1 at the destination D is

$$\frac{1}{2}I(X^1; y_{D_1}, y_{D_2}|X^0) = \frac{1}{2}\log_2 \left(1 + \frac{P_s^1 |\alpha_0|^2}{N_0} + \frac{\psi^* \alpha^* \alpha \psi}{N_0} \right). \quad (9)$$

Using (3), (5), and assuming the knowledge of X^0 at the eavesdroppers, the information rate for X^1 at eavesdropper E_j is

$$\frac{1}{2}I(X^1; y_{E_{1j}}, y_{E_{2j}}|X^0) = \frac{1}{2}\log_2 \left(1 + \frac{P_s^1 |\beta_{0j}|^2}{N_0} + \frac{\psi^* \beta_j^* \beta_j \psi}{N_0} \right). \quad (10)$$

We note that there is no decoding constraint for the symbol X^0 on any eavesdropper E_j similar to (6) and (7). This makes (10) as the best possible information rate for symbol X^1 at E_j . Further, with the knowledge of symbol X^0 , the relays will be able to decode the symbol X^1 if $\forall i = 1, 2, \dots, N$ [12,15]

$$\frac{1}{2}I(X^1; y_{R_i}|X^0) \geq \frac{1}{2}I(X^1; y_{D_1}, y_{D_2}|X^0), \quad (11)$$

i.e.,

$$\frac{1}{2}\log_2 \left(1 + \frac{P_s^1 |\gamma_i|^2}{N_0} \right) \geq \frac{1}{2}\log_2 \left(1 + \frac{P_s^1 |\alpha_0|^2}{N_0} + \frac{\psi^* \alpha^* \alpha \psi}{N_0} \right). \quad (12)$$

The constraint on the total transmit power is

$$P_s^0 + P_s^1 + \phi^* \phi + \psi^* \psi \leq P_T. \quad (13)$$

Subject to the constraints in (6), (7), (12), and (13), the worst case achievable secrecy rate for X^1 is obtained by solving the following optimization problem [7,12,15]:

$$R_s = \max_{P_s^0, P_s^1, \phi, \psi} \min_{j:1,2,\dots,J} \left\{ \frac{1}{2} I(X^1; y_{D_1}, y_{D_2} | X^0) - \frac{1}{2} I(X^1; y_{E_{1j}}, y_{E_{2j}} | X^0) \right\}^+, \quad (14)$$

s.t.

$$\frac{1}{2} I(X^0; y_{R_i}) \geq R_0, \quad \forall i = 1, 2, \dots, N, \quad (15)$$

$$\frac{1}{2} I(X^0; y_{D_1}, y_{D_2}) \geq R_0, \quad (16)$$

$$\frac{1}{2} I(X^1; y_{R_i} | X^0) \geq \frac{1}{2} I(X^1; y_{D_1}, y_{D_2} | X^0), \quad \forall i = 1, 2, \dots, N, \quad (17)$$

$$P_s^0 \geq 0, P_s^1 \geq 0, P_s^0 + P_s^1 + \phi^* \phi + \psi^* \psi \leq P_T, \quad (18)$$

where $\{a\}^+ = \max(a, 0)$, and without loss of generality we drop this operator since secrecy rate is non-negative. The constraints (15), (16), and (17) are obtained from (6), (7), and (12), respectively. The objective function in (14) is obtained from (9) and (10). We solve the optimization problem in (14) as follows.

Step1 : Divide the total available transmit power P_T in M discrete steps of size $\Delta_{P_T} = \frac{P_T}{M}$, and let $P_m = m\Delta_{P_T}$, where $m = 0, 1, 2, \dots, M-1$.

Step2 : Rewrite the optimization problem (14) as the following two separate optimization problems; Problem 1 and Problem 2.

Problem 1:

$$\max_{P_s^1, \psi} \min_{j:1,2,\dots,J} \frac{1}{2} \left\{ \log_2 \left(1 + \frac{P_s^1 |\alpha_0|^2 + \psi^* \alpha^* \alpha \psi}{N_0} \right) - \log_2 \left(1 + \frac{P_s^1 |\beta_{0j}|^2 + \psi^* \beta_j^* \beta_j \psi}{N_0} \right) \right\}, \quad (19)$$

s.t.

$$\forall i = 1, 2, \dots, N, \quad \frac{1}{2} \log_2 \left(1 + \frac{P_s^1 |\gamma_i|^2}{N_0} \right) \geq \frac{1}{2} \log_2 \left(1 + \frac{P_s^1 |\alpha_0|^2 + \psi^* \alpha^* \alpha \psi}{N_0} \right), \quad P_s^1 \geq 0, \quad P_s^1 + \psi^* \psi \leq P_m. \quad (20)$$

The optimization problem in (19) is a function of P_s^1 , ψ , and P_m . For a given P_m , it can be solved using semi-definite relaxation technique in [15].

Problem 2:

$$\text{find } P_s^0, \phi, \quad (21)$$

$$\begin{aligned} & \text{s.t. } \forall i = 1, 2, \dots, N, \\ & \frac{1}{2} \log_2 \left(1 + \frac{P_s^0 |\gamma_i|^2}{N_0 + P_s^1 |\gamma_i|^2} \right) \geq R_0, \\ & \frac{1}{2} \log_2 \left(1 + \frac{P_s^0 |\alpha_0|^2}{N_0 + P_s^1 |\alpha_0|^2} + \frac{\phi^* \alpha^* \alpha \phi}{N_0 + \psi^* \alpha^* \alpha \psi} \right) \geq R_0, \\ & P_s^0 \geq 0, P_s^0 + \phi^* \phi \leq P_T - P_m. \end{aligned} \quad (22)$$

For a given P_s^1 , ψ , and P_m , it is obvious that the optimum direction of ϕ which minimizes the transmit power $P_s^0 + \phi^* \phi$, subject to the constraints in (22), lies in the direction of α^* , i.e., $\phi = \sqrt{P_R^0} \phi_u$, where $\phi_u = \frac{\alpha^*}{\|\alpha^*\|}$ and P_R^0 is the relays transmit power associated with X_0 . With this, we rewrite the feasibility problem in (21) in the following form:

$$\text{find } P_s^0, P_R^0, \quad (23)$$

s.t.

$$\begin{aligned} & \left(1 + \frac{P_s^0 |\gamma_i|^2}{N_0 + P_s^1 |\gamma_i|^2} \right) \geq 2^{2R_0}, \quad \forall i = 1, 2, \dots, N, \\ & \left(1 + \frac{P_s^0 |\alpha_0|^2}{N_0 + P_s^1 |\alpha_0|^2} + \frac{P_R^0 \phi_u^* \alpha^* \alpha \phi_u}{N_0 + \psi^* \alpha^* \alpha \psi} \right) \geq 2^{2R_0}, \\ & P_s^0 \geq 0, P_R^0 \geq 0, P_s^0 + P_R^0 \leq P_T - P_m. \end{aligned} \quad (24)$$

For a given P_s^1 , ψ , and P_m , the feasibility problem in (23) with its constraints in (24) is a linear feasibility problem in P_s^0 and P_R^0 , and it can be easily solved using linear programming techniques.

It can be shown that the secrecy rate R_s^m which is obtained by solving the optimization problem (19) for a given P_m is a strictly increasing function in P_m [15]. Hence, the idea is to find the maximum power P_m for which P_s^1 and ψ obtained by solving (19) also gives a feasible solution P_s^0 and P_R^0 in (23) satisfying the constraints in (24). This can be achieved by decreasing m from $M-1$ towards 0 and finding the maximum m for which the solution of the optimization problem (19) (i.e., P_s^1 , ψ) with P_m as available power also gives a feasible solution for (23) (i.e., P_s^0 and P_R^0 satisfying the constraints in (24)).

A. Suboptimal beamforming with non-secret message for D and all E_j s

In this subsection, we give a suboptimal beamforming method with secret and non-secret messages where the secret message W_1 is intended only for D whereas the non-secret message W_0 is intended for D as well as all E_j s. The non-secret message is transmitted at a fixed rate R_0 . Similar to (7), using (3), (5) and treating X^1 as noise, E_j s will be able to decode X^0 if $\forall j = 1, 2, \dots, J$,

$$\begin{aligned} \frac{1}{2} I(X^0; y_{E_{1j}}, y_{E_{2j}}) &= \frac{1}{2} \log_2 \left(1 + \frac{P_s^0 |\beta_{0j}|^2}{N_0 + P_s^1 |\beta_{0j}|^2} + \frac{\phi^* \beta_j^* \beta_j \phi}{N_0 + \psi^* \beta_j^* \beta_j \psi} \right) \geq R_0. \end{aligned} \quad (25)$$

With this, the optimization problem in (14) will have additional constraints (25). Similarly, the feasibility problem (21) will

have the additional constraints (25). For a given P_s^1 , ψ , and P_m , the optimum direction of ϕ which minimizes the transmit power $P_s^0 + \phi^* \phi$, can be obtained by solving the following optimization problem:

$$\begin{aligned} \min_{P_s^0, \Phi} \quad & P_s^0 + \text{trace}(\Phi), \quad (26) \\ \text{s.t.} \quad & \forall i = 1, 2, \dots, N, \\ & \left(1 + \frac{P_s^0 |\gamma_i|^2}{N_0 + P_s^1 |\gamma_i|^2}\right) \geq 2^{2R_0}, \\ & \left(1 + \frac{P_s^0 |\alpha_0|^2}{N_0 + P_s^1 |\alpha_0|^2} + \frac{\alpha \Phi \alpha^*}{N_0 + \psi^* \alpha^* \alpha \psi}\right) \geq 2^{2R_0}, \\ & \left(1 + \frac{P_s^0 |\beta_{0j}|^2}{N_0 + P_s^1 |\beta_{0j}|^2} + \frac{\beta_j \Phi \beta_j^*}{N_0 + \psi^* \beta_j^* \beta_j \psi}\right) \geq 2^{2R_0}, \\ & \forall j = 1, 2, \dots, J, \quad \Phi \succeq \mathbf{0}, \quad \text{rank}(\Phi) = 1, \\ & P_s^0 \geq 0, \quad P_s^0 + \text{trace}(\Phi) \leq P_T - P_m, \quad (27) \end{aligned}$$

where $\Phi = \phi \phi^*$ and the constraints in (27) are written using all the constraints in (22) and (25). This is a non-convex optimization problem which is difficult to solve. However, by relaxing the $\text{rank}(\Phi) = 1$ constraint, the above problem can be solved using semi-definite programming techniques. But, the solution Φ of the above rank relaxed optimization problem may not have rank 1. So, we take the largest eigen direction of Φ as the suboptimal unit norm direction ϕ_u . We substitute ϕ_u in the feasibility problem (23) and its constraints (24) and additional constraints (25). The remaining procedure to find P_s^0 , P_s^1 , P_R^0 and ψ remains same as discussed in **Step1** and **Step2**.

IV. BEAMFORMING WITH SECRET AND NON-SECRET MESSAGES – STATISTICAL CSI ON EAVESDROPPERS LINKS

In this section, we obtain the source and relays powers under the assumption that only the statistical knowledge of the eavesdroppers CSI is available. The eavesdropper CSI is assumed to be iid $\mathcal{CN}(0, \sigma_{\beta_{0j}}^2)$ for the direct link from source to E_j and iid $\mathcal{CN}(0, \sigma_{\beta_{ij}}^2)$ for the link from relay i to E_j . With this statistical knowledge of the eavesdroppers CSI, the optimization problem (19) can be written in the following form:

$$\begin{aligned} \max_{P_s^1, \psi} \min_{j:1,2,\dots,J} \quad & R_s^m = \frac{1}{2} \left\{ \log_2 \left(1 + \frac{P_s^1 |\alpha_0|^2 + \psi^* \alpha^* \alpha \psi}{N_0} \right) \right. \\ & \left. - \mathbb{E} \left[\log_2 \left(1 + \frac{P_s^1 |\beta_{0j}|^2 + \psi^* \beta_j^* \beta_j \psi}{N_0} \right) \right] \right\} \quad (28) \\ \geq \\ \max_{P_s^1, \psi} \min_{j:1,2,\dots,J} \quad & \frac{1}{2} \left\{ \log_2 \left(1 + \frac{P_s^1 |\alpha_0|^2 + \psi^* \alpha^* \alpha \psi}{N_0} \right) \right. \\ & \left. - \log_2 \left(1 + \frac{P_s^1 \sigma_{\beta_{0j}}^2 + \psi^* \Lambda_{\beta_j} \psi}{N_0} \right) \right\}, \quad (29) \end{aligned}$$

$$\begin{aligned} \text{s.t.} \quad & \forall i = 1, 2, \dots, N, \quad \frac{1}{2} \log_2 \left(1 + \frac{P_s^1 |\gamma_i|^2}{N_0} \right) \geq \\ & \frac{1}{2} \log_2 \left(1 + \frac{P_s^1 |\alpha_0|^2 + \psi^* \alpha^* \alpha \psi}{N_0} \right), \\ & P_s^1 \geq 0, \quad P_s^1 + \psi^* \psi \leq P_m, \quad (30) \end{aligned}$$

where the lower bound in (29) is due to Jensen's inequality. The Λ_{β_j} in (29) is a diagonal matrix with $[\sigma_{\beta_{1j}}^2, \sigma_{\beta_{2j}}^2, \dots, \sigma_{\beta_{Nj}}^2]^T$ on its diagonal. For a given P_m , the optimization problem (29) can be solved using semi-definite relaxation. The optimal P_s^0 , P_s^1 , P_R^0 , and ψ can be obtained by solving the optimization problems (29) and (23) as discussed in Section-III.

V. RESULTS AND DISCUSSIONS

We present the numerical results and discussions in this section. We obtained the secrecy rate results through simulations for $N = 2$ relays and $J = 1, 2, 3$ eavesdroppers. The following complex channel gains are taken in the simulations: $\alpha_0 = 0.3039 + 0.5128i$, $\beta_{01} = 0.1161 - 0.0915i$, $\beta_{02} = -0.5194 + 0.4268i$, $\beta_{03} = -0.0900 + 0.4769i$, $\gamma = [-1.3136 + 0.3534i, -0.7070 - 1.1305i]$, $\alpha = [0.3241 + 0.4561i, 0.2713 - 0.5850i]$, $\beta_1 = [-0.6407 + 0.0709i, -0.0562 + 0.5120i]$, $\beta_2 = [0.1422 - 0.6060i, -0.0590 - 0.3308i]$, and $\beta_3 = [0.2793 - 0.1426i, -0.5092 + 0.2570i]$. For the case of statistical CSI on eavesdroppers links, the following parameters are taken: $\sigma_{\beta_{01}}^2 = 0.01$, $\sigma_{\beta_{02}}^2 = 0.04$, $\sigma_{\beta_{03}}^2 = 0.09$, $\sigma_{\beta_{i1}}^2 = 0.25$, $\sigma_{\beta_{i2}}^2 = 0.36$, $\sigma_{\beta_{i3}}^2 = 0.49$, $i = 1, 2$. The value of M is taken to be 50.

Perfect CSI on all Links: Figure 2(a) shows the secrecy rate plots for DF relay beamforming as a function of total transmit power (P_T) for the case when perfect CSI on all links is assumed. The secrecy rates are plotted for the cases of with and without W_0 for 2 relays and different number of eavesdroppers. For the case with W_0 , the information rate of the W_0 is fixed at $R_0 = 0.2$. We also assume that when W_0 is present, it is intended only for D and it need not be protected from E_j s. From Fig. 2(a), we observe that, for a given number of eavesdroppers, the secrecy rate degrades when W_0 is present. However, this degradation becomes insignificant when P_T is increased to large values. Also, the secrecy rate degrades for increasing number of eavesdroppers. Figure 2(b) shows the R_s vs R_0 tradeoff, where R_s is plotted as a function of R_0 for $J = 1, 2, 3$ at a fixed total power of $P_T = 6$ dB. It can be seen that as R_0 is increased, secrecy rate decreases. This is because the available transmit power for W_1 decreases as R_0 is increased. In Fig. 2(b), we see that the maximum achievable secrecy rate R_s without W_0 (i.e., when $R_0 = 0$), which we denote by R'_s , are 0.58, 0.45 and 0.28 for $J = 1, 2, 3$ eavesdroppers, respectively. It can be further noted that if $R_0 \leq R'_s$, then W_0 can also be transmitted as a secret message and the remaining rate $R'_s - R_0$ can be used for the secret message (W_1) transmission. In other words, if $R_0 \leq R'_s$, then it is possible for both W_1 and W_0 to be sent as secret message

at a combined secrecy rate R'_s . However, if $R_0 > R'_s$, then W_0 can not be transmitted as a secret message.

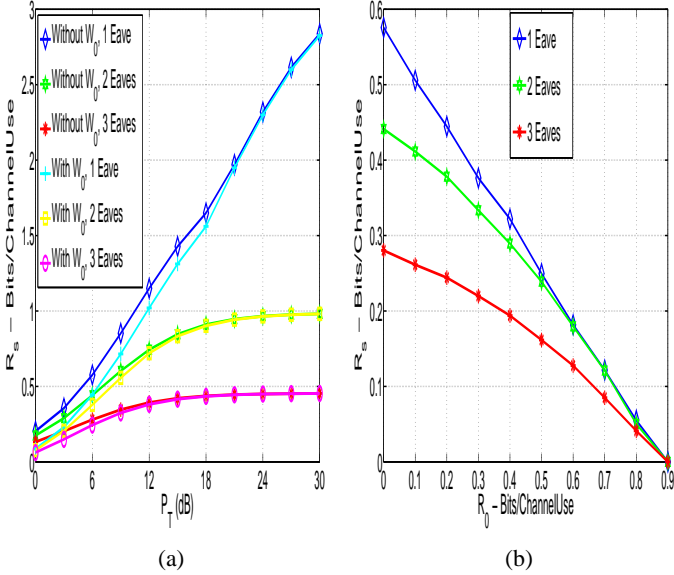


Fig. 2. Secrecy rate of DF relay beamforming for $N = 2$, $J = 1, 2, 3$. Perfect CSI on all links. (a) secrecy rate vs total power (P_T) with and without W_0 , $R_0 = 0.2$; (b) R_s vs R_0 for $P_T = 6$ dB.

Statistical CSI on eavesdroppers links: Figures 3(a) and (b) show the secrecy rate plots for DF relay beamforming for the case when only the statistical CSI on eavesdroppers links is assumed to be known. The CSI on the other links are assumed to be perfectly known. Figure 3(a) shows the secrecy rate versus P_T plots for $R_0 = 0.2$, and Fig. 3(b) shows the secrecy rate versus R_0 plots for $P_T = 6$ dB. Observations similar to those in the case of perfect CSI on all links are observed in Figs. 3(a) and 3(b) as well.

VI. CONCLUSIONS

We investigated beamforming in DF relaying using multiple relays, where the source sends a secret message as well as a non-secret message to the destination node in the presence of multiple non-colluding eavesdroppers. The source and relays operate under a total power constraint. We obtained the optimum source powers and weights of the relays for both secret and non-secret messages which maximized the worst case secrecy rate for the secret message as well as met the information rate constraint R_0 for the non-secret message. We solved this problem for the cases when (i) perfect CSI of all links was known, and (ii) only the statistical CSI of the eavesdroppers links and perfect CSI of other links were known.

REFERENCES

- [1] A. Wyner, "The wire-tap channel," *Bell. Syst. Tech. J.*, vol. 54, no. 8, pp. 1355-1387, Jan. 1975.
- [2] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 339-348, May 1978.

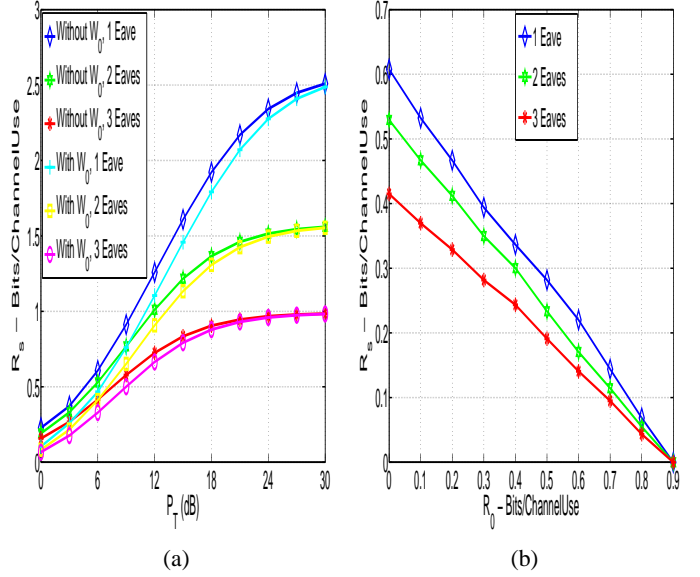


Fig. 3. Secrecy rate of DF relay beamforming for $N = 2$, $J = 1, 2, 3$. Statistical CSI on eavesdroppers links. (a) secrecy rate vs P_T with and without W_0 , $R_0 = 0.2$; (b) R_s vs R_0 for $P_T = 6$ dB.

- [3] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 451-456, Jul. 1978.
- [4] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information theoretic security," *Foundations and Trends in Communications and Information Theory*, NOW Publishers, vol. 5, no. 4-5, 2009.
- [5] A. Khisti and G. Wornell, "Secure transmission with multiple antennas-I: The MISOME wiretap channel," *IEEE Trans. Inform. Theory*, vol. 56, no. 7, pp. 3088-3104, Jul. 2010.
- [6] A. Khisti and G. Wornell, "Secure transmission with multiple antennas-II: The MIMOME wiretap channel," *IEEE Trans. Inform. Theory*, vol. 56, no. 11, pp. 5515-5532, Nov. 2010.
- [7] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai, "Compound wiretap channels," *EURASIP Journ. on Wireless Commun. and Net.*, volume 2009, article ID 142374, 12 pages. doi:10.1155/2009/142374
- [8] H. D. Ly, T. Liu, and Y. Liang, "Multiple-input multiple-output Gaussian broadcast channels with common and confidential messages," *IEEE Trans. Inform. Theory*, vol. 56, no. 11, pp. 5477-5487, Nov. 2010.
- [9] E. Ekrem and S. Ulukus, "Capacity region of Gaussian MIMO broadcast channels with common and confidential messages," *IEEE Trans. Inform. Theory*, vol. 58, no. 9, pp. 5669-5680, Sept. 2012.
- [10] R. Liu, T. Liu, and H. V. Poor, "New results on multiple-input multiple-output broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 59, no. 3, pp. 1346-1359, Mar. 2013.
- [11] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inform. Theory*, vol. 54, no. 9, pp. 4005-4019, Sep. 2008.
- [12] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875-1888, Mar. 2010.
- [13] J. Zhang and M. C. Gursoy, "Collaborative relay beamforming for secrecy," *Proc. IEEE ICC'2010*, Cape Town, May 2010.
- [14] J. Li, A. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4985-4997, Oct. 2011.
- [15] S. Vishwakarma and A. Chockalingam, "Decode-and-forward relay beamforming for secrecy with finite-alphabet input," *IEEE Commun. Letters*, vol. 17, no. 5, pp. 912-915, May 2013.
- [16] S. Boyd and L. Vandenberghe, *Convex optimization*, Cambridge Univ. Press, 2004.